ILUSTRE COLEGIO
DE LA ABOGACÍA
DE MADRID

Pliego técnico de la licitación para la contratación de las soluciones tecnológicas para RGPD y NOTIFICACIONES

29 de abril de 2026

Todas las referencias a trabajador, empleado, abogado, letrado, persona colegiada, usuario, así como a cualesquiera cargos o referencias en que se utilice el masculino, se entenderán en contenido semántico neutro, luego comprensivas de cualquier condición sexual o identidad

ÍNDICE

Control de Versiones

Versión	Fecha	Comentarios	Páginas Afectadas
1	21/04/2026	Original	Todas

1. OBJETO

El Ilustre Colegio de la Abogacía de Madrid (ICAM) se encuentra inmerso en un proceso de transformación digital orientado a la modernización de sus sistemas, la mejora de la eficiencia operativa y la adaptación a un entorno cada vez más exigente desde el punto de vista normativo, tecnológico y de relación con los usuarios.

En este contexto, resulta necesario evolucionar hacia un modelo integrado que permita gestionar de forma coherente y transversal tanto la **protección de datos personales** como los **sistemas de notificaciones y comunicaciones**.

El objeto del presente contrato es la definición, diseño, desarrollo, implantación e integración de dos soluciones tecnológicas diferenciadas dentro del ecosistema del ICAM, orientadas a mejorar la gestión, la trazabilidad y el cumplimiento normativo en los ámbitos de la protección de datos personales (RGPD) y de las notificaciones y comunicaciones.

En concreto, el contrato tiene por finalidad, por un lado, la implantación de un sistema corporativo centralizado que garantice el cumplimiento del Reglamento General de Protección de Datos (RGPD), mediante la gestión estructurada de los tratamientos de datos personales, las cláusulas informativas y los consentimientos, asegurando su trazabilidad, control y alineación con la normativa vigente. Por otro lado, la implantación de una sede electrónica de notificaciones y comunicaciones que permita la gestión integral de los envíos dirigidos a los usuarios del ICAM, garantizando su correcta ejecución, trazabilidad, generación de evidencias y, en su caso, su validez jurídica.

Ambas soluciones deberán integrarse con la arquitectura tecnológica del ICAM, garantizando su interoperabilidad, seguridad, escalabilidad y coherencia funcional, si bien responden a necesidades y procesos de negocio claramente diferenciados.

2. ALCANCE

El alcance del presente contrato comprende todas las actividades necesarias para la correcta ejecución de los dos procesos objeto de la licitación, incluyendo el análisis, diseño funcional y técnico, desarrollo, configuración, integración, pruebas, implantación y soporte, diferenciando expresamente el ámbito de cada uno de ellos.

2.1 Alcance del proyecto de RGPD

El alcance del proyecto de RGPD comprende la implantación de un modelo corporativo centralizado de cumplimiento en materia de protección de datos, basado en la gestión estructurada de los tratamientos, las cláusulas informativas y los consentimientos, así como en su integración con los sistemas corporativos existentes.

En particular, el alcance comprende la definición, implantación y adopción de un Sistema Centralizado de Gestión de Tratamientos y Consentimientos (SCGTC), que actuará como autoridad funcional y técnica en esta materia dentro del ecosistema del ICAM.

Este modelo será de aplicación obligatoria a todas las iniciativas tecnológicas del Colegio que impliquen tratamiento de datos personales, tanto nuevas como evoluciones de sistemas existentes, garantizando el cumplimiento del principio de privacidad desde el diseño y por defecto.

Hay que destacar que la implementación relativa a la protección de datos tendrá carácter transversal, afectando a todos los procesos del ICAM en los que se traten datos personales.

Se deberá garantizar la coherencia con el Registro de Actividades de Tratamiento, la gestión del ciclo de vida del dato, el soporte al ejercicio de los derechos de los interesados y la correcta integración del modelo de protección de datos en la arquitectura tecnológica del ICAM, así como el cumplimiento y adaptación a la normativa, en concreto al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD), la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y demás normativa aplicable, en el ámbito del ICAM.

El Sistema Centralizado de Gestión de Tratamientos y Consentimientos (SCGTC) actuará como autoridad funcional y técnica en materia de gobierno del dato dentro del ICAM, siendo el punto único obligatorio para la gestión de tratamientos, bases jurídicas y consentimientos

El alcance incluye la definición de reglas operativas de propagación, gestión de inconsistencias y mecanismos de resiliencia para garantizar la integridad del dato entre todos los sistemas integrados

2.2 Alcance del proyecto de Notificaciones

El alcance del proyecto de Notificaciones y Comunicaciones comprende la implantación de una sede electrónica que permita la gestión integral del ciclo de vida de los envíos dirigidos a los usuarios del ICAM.

Este alcance incluye la generación, gestión, envío y consulta de notificaciones y comunicaciones, diferenciando aquellas con efectos jurídicos de las meramente informativas, así como la gestión de envíos tanto individuales como masivos y multicanal (electrónicos y, en su caso, postales).

Asimismo, se contempla la trazabilidad completa del proceso, desde la puesta a disposición hasta el acceso por parte del destinatario, incluyendo la generación y custodia de evidencias electrónicas, la gestión de plazos y la integración con servicios externos de certificación.

El sistema deberá proporcionar un punto único de acceso para los usuarios, permitir la automatización de envíos mediante reglas de negocio y garantizar su alineación con el modelo de protección de datos, especialmente en lo relativo a preferencias, consentimientos y tratamiento de la información personal.

3. DETALLE FUNCIONAL

3.1 Proceso RGPD

A continuación, se detalla, a nivel funcional, el proceso de gestión de tratamientos y consentimientos en el marco del RGPD del ICAM, definiendo su operativa, los requisitos asociados y los elementos necesarios para garantizar su correcta implantación, control y cumplimiento dentro del sistema.

El sistema deberá configurarse como un componente estructural dentro de la arquitectura tecnológica del ICAM, actuando como repositorio maestro y fuente única de referencia en materia de tratamientos y consentimientos.

El adjudicatario deberá definir y documentar las políticas de gestión de errores, los mecanismos de reintento automático, el almacenamiento temporal y los criterios de consistencia eventual, especialmente en lo relativo a las sincronizaciones entre sistemas.

Asimismo, deberá contemplarse la definición de los principios y requisitos que deban incorporarse en el diseño de cualquier solución tecnológica que implique tratamiento de datos personales, asegurando su alineación con el Registro de Actividades de Tratamiento (RAT) y con el modelo de gobierno del dato del Colegio.

Cabe destacar que, por su naturaleza transversal, la solución deberá integrarse en todos los procesos e iniciativas del ICAM, afectando tanto a los sistemas existentes como a los nuevos desarrollos, y garantizando:

- La identificación previa de los tratamientos en cualquier desarrollo.
- La correcta información al interesado mediante cláusulas informativas.
- La adecuada gestión de las bases jurídicas.
- La trazabilidad completa de las acciones realizadas sobre los datos.

El Sistema Centralizado de Gestión de Tratamientos y Consentimientos (SCGTC) es un sistema que permite implementar de forma efectiva las obligaciones del RGPD mediante la centralización, estructuración y control de la información relativa a los tratamientos de datos personales, sus bases jurídicas y las evidencias asociadas, especialmente el consentimiento.

A tal efecto, deberán aplicarse las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento es conforme con el RGPD.

Las características principales del Sistema Centralizado de Gestión de Tratamientos y Consentimientos, que deberán cumplirse con la implementación de la solución objeto del presente proyecto, son las siguientes:

- Centralización del gobierno del dato

Deberá garantizarse la responsabilidad y capacidad de control del responsable del tratamiento, permitiendo la gestión en un único sistema del inventario de tratamientos, las bases jurídicas asociadas a cada uno de ellos y las evidencias correspondientes.

- Gestión del consentimiento conforme al RGPD

El sistema deberá garantizar que el consentimiento cumpla con los requisitos establecidos en la normativa aplicable, y en particular que sea libre, específico, informado e inequívoco, así como demostrable y revocable en cualquier momento.

- Trazabilidad y evidencias

Deberá garantizarse la trazabilidad completa y el registro de evidencias, permitiendo conocer en todo momento quién, cuándo y cómo se obtuvo el consentimiento, qué información y cláusulas fueron mostradas al interesado, así como la versión de las mismas vigente en el momento de su otorgamiento.

- Registro de actividades de tratamiento (RAT)

El Colegio dispone de un Registro de Actividades de Tratamiento (RAT), que constituye el instrumento formal mediante el cual se documentan y estructuran todas las actividades de tratamiento realizadas en calidad de responsable. Dicho registro deberá incluir, al menos, la siguiente información:

a) El nombre y los datos de contacto del responsable

b) Los fines del tratamiento

c) Una descripción de las categorías de interesados y de las categorías de datos personales

d) Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales

e) En su caso, las transferencias de datos personales a un tercer país o una organización internacional

f) Los plazos previstos para la supresión de las diferentes categorías de datos

g) Una descripción general de las medidas técnicas y organizativas de seguridad

- Privacidad desde el diseño y por defecto

Deberán aplicarse medidas técnicas y organizativas apropiadas que garanticen que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada finalidad específica. Esta obligación se aplicará a la cantidad de datos recogidos, al alcance del tratamiento, a los plazos de conservación y a la accesibilidad de los datos. Ello implicará una configuración por defecto orientada a la protección de datos y la realización de evaluaciones previas de riesgos.

- Integración con sistemas corporativos del ICAM

La solución deberá integrarse con los sistemas corporativos del ICAM, permitiendo la consulta del estado del consentimiento por parte de otros sistemas y garantizando la coherencia en todos los canales, evitando posibles incumplimientos derivados de sistemas no integrados.

- Gestión del ciclo de vida

Deberá gestionarse el ciclo de vida de los datos conforme a los requisitos normativos aplicables, garantizando el principio de limitación del plazo de conservación. Esta gestión incluirá, entre otras actuaciones, la creación y modificación de tratamientos, los cambios en las bases jurídicas que los sustentan, la actualización de la información y la supresión o eliminación de los datos.

- Seguridad y control de accesos

Deberá garantizarse un nivel de seguridad adecuado al riesgo, incluyendo mecanismos de control de accesos y registro de actividad.

A tal efecto, se deberá establecer un proceso de verificación, evaluación y valoración periódica de la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

Asimismo, deberán implementarse medidas que permitan restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

Se valorará la aplicación de técnicas de seudonimización y cifrado de los datos personales cuando resulte adecuado.

- Soporte a derechos de los interesados

Deberán implementarse herramientas que faciliten el ejercicio de los derechos de los interesados: acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y el derecho a no ser objeto de decisiones automatizadas, incluida la elaboración de perfiles, garantizando en todo caso la transparencia y el control por parte del interesado.

3.1.1 REQUERIMIENTOS

Teniendo en cuenta todo lo anteriormente expuesto, y considerando que deberá integrarse en el desarrollo del SCGTC, se especifican a continuación los requisitos que deberán cumplirse para el diseño, desarrollo e implementación del Sistema Centralizado de Gestión de Tratamientos y Consentimientos.

Como premisa general, deberá contemplarse que el SCGTC se implemente diferenciando claramente los siguientes ámbitos funcionales:

- **Front office (Área de Preferencias)**

Interfaz unificada dirigida al interesado (persona colegiada/usuario), que permitirá la consulta de los tratamientos aplicables y la gestión de sus consentimientos (otorgamiento, aceptación y, en su caso, revocación), cuando proceda.

- Back office (Gobierno)

Interfaz interna destinada a la gestión del ciclo de vida de los tratamientos y las cláusulas (alta, modificación y versionado), que deberá incorporar flujos de revisión y aprobación por parte de las áreas competentes (Seguridad de la Información y Calidad, así como DPD/Servicios Jurídicos), garantizando en todo momento la trazabilidad completa de las actuaciones.

Gobierno y cumplimiento.

Este ámbito establece el marco normativo, el modelo de datos y las reglas de control que rigen el sistema. Constituye la base necesaria para el diseño, implementación y validación del resto de las capacidades del SCGTC, garantizando su conformidad con el RGPD.

RQ.0 – Identificación de tratamiento

Toda funcionalidad, proceso o iniciativa que implique el tratamiento de datos personales deberá identificar previamente el tratamiento al que se vincula o, en su caso, justificar la creación o modificación de uno existente en el SCGTC.

Con carácter previo a la aprobación funcional o técnica de cualquier desarrollo, deberá realizarse, completarse y documentarse la siguiente evaluación:

- Determinar si la iniciativa implica tratamiento de datos personales
- Identificar si se trata de un nuevo tratamiento o de la modificación de uno existente
- Verificar su encaje en el Registro de Actividades de Tratamiento (RAT)
- Definir la base jurídica que legitima el tratamiento
- Evaluar si procede la obtención de consentimiento
- Determinar si es necesaria la creación o actualización de una versión de cláusula informativa
- Confirmar la integración obligatoria con el Sistema Centralizado de Gestión de Tratamientos y Consentimientos (SCGTC)
- Determinar si debe registrarse la visualización de cláusula, la aceptación expresa o ambas

Toda evaluación previa deberá documentar explícitamente la relación entre el tratamiento principal y sus posibles subtratamientos o finalidades derivadas, garantizando su coherencia con el Registro de Actividades de Tratamiento (RAT).

La presente evaluación constituye un requisito previo de diseño y deberá quedar formalmente documentada y validada por el área de Seguridad de la Información y Calidad antes de la aprobación de la iniciativa.

RQ.1 – Gestión de tratamientos

La gestión de los tratamientos deberá permitir, al menos, las siguientes funcionalidades:

- Permitir la creación, modificación y baja de tratamientos de datos personales, incluyendo la gestión de todos sus atributos asociados (finalidad, base jurídica, categorías de datos, categorías de interesados, destinatarios, plazos de conservación, entre otros).

- Deberá implementarse un sistema de versionado histórico de los tratamientos, que distinga entre:

    - Cambios informativos.

      Aquellos que generen una nueva versión del tratamiento sin afectar a la validez de los consentimientos previamente otorgados, ni requerir la obtención de un nuevo consentimiento.

    - Cambios sustanciales.

      Aquellos que generen una nueva versión del tratamiento y conlleven que los consentimientos previamente otorgados pasen a estado de "pendiente de renovación". Hasta que el interesado renueve su consentimiento, los tratamientos basados en dicha base jurídica deberán quedar suspendidos. En estos casos, será obligatoria la obtención de un nuevo consentimiento.

- Deberá garantizarse la coherencia y sincronización con el Registro de Actividades de Tratamiento (RAT).

A estos efectos, el SCGTC será considerado la fuente operativa única (*Golden Source*) para la información relativa a tratamientos (incluyendo versiones, bases jurídicas y vigencias), mientras que el RAT actuará como repositorio de carácter documental y de referencia formal.

En caso de discrepancia entre ambos sistemas, prevalecerá la información contenida en el SCGTC, salvo resolución formal adoptada de forma conjunta por el Delegado de Protección de Datos y el área de Seguridad de la Información.

RQ.2 – Modelo de datos y trazabilidad

El modelo de datos deberá contemplar la definición estructurada de tratamientos, sus versiones y los consentimientos asociados.

A tal efecto, deberá emplearse un modelo de datos que garantice:

- Integridad referencial y gobernanza de datos en el entorno corporativo.
- Copias de seguridad, continuidad y operación alineadas con los estándares TI.
- Segregación lógica (permisos por esquema/tablas) entre gobierno y consumo.

En la fase de diseño detallado del Sistema Centralizado de Gestión de Tratamientos y Consentimientos (SCGTC), se deberá definir el modelo lógico y físico de datos que soporte su funcionamiento. Dicho diseño deberá dar respuesta, al menos, a las siguientes necesidades:

- Separar la definición del tratamiento de sus distintas versiones.
- Permitir la gestión granular de bases jurídicas y consentimientos.
- Garantizar la trazabilidad histórica de modificaciones.
- Asegurar la integridad de la evidencia asociada a los consentimientos.
- Facilitar la interoperabilidad con el Registro de Actividades de Tratamiento
- Integrar los requisitos de control y auditoría derivados del ENS y del SGSI.

Asimismo, deberá mantenerse un histórico completo de la información, sin pérdida de datos.

El sistema deberá registrar los consentimientos con granularidad transaccional, incluyendo, al menos, los siguientes estados: pendiente, procesado, error, reconciliado, así como cualquier otro estado intermedio que resulte necesario para garantizar la correcta gestión del ciclo de vida.

El adjudicatario deberá implementar un mecanismo de detección, registro y gestión de inconsistencias, que incluya procesos de reconciliación tanto automáticos como manuales, bajo la supervisión del área de Seguridad de la Información.

Ciclo de vida del consentimiento

Este bloque define el núcleo funcional del sistema, abarcando la creación, gestión, versionado y revocación de consentimientos y cláusulas, en coherencia con las bases jurídicas aplicables y los requisitos de trazabilidad exigidos.

El SCGTC deberá permitir la gestión de consentimientos de forma granular, así como su agrupación y anidamiento, incluyendo la definición de jerarquías de finalidades y dependencias entre tratamientos.

RQ.3 – Gestión de cláusulas informativas

La gestión de cláusulas informativas deberá contemplar, al menos, los siguientes aspectos:

- Gestión de cláusulas.

  Permitir la creación, versionado y gestión de cláusulas informativas, garantizando su correcta vinculación con los tratamientos correspondientes.

- Publicación de cláusulas.

  Permitir la exposición y disponibilidad de las cláusulas vigentes a los sistemas consumidores (sitios web, aplicaciones, formularios u otros canales), garantizando el acceso a la versión aplicable en cada contexto).

- Versionado de cláusulas.

  Implementar un sistema de versionado que permita la gestión de distintas versiones de las cláusulas, con control de su vigencia, histórico y trazabilidad completa.

La plataforma deberá permitir el versionado paralelo de cláusulas en distintos idiomas, garantizando la trazabilidad independiente por cada versión e idioma, así como su correcta asociación a los tratamientos y contextos de uso correspondientes.

RQ.4 – Gestión de consentimientos

- Registro de consentimiento.

  Permitir la captura del consentimiento, garantizando su vinculación con el tratamiento correspondiente y con la versión concreta de la cláusula informativa aplicada.

- Revocación de consentimiento.

  Permitir la revocación del consentimiento en cualquier momento, con efectos inmediatos sobre los tratamientos que se fundamenten en dicha base jurídica.

- Trazabilidad de consentimientos.

  Garantizar el registro completo de evidencias asociadas al consentimiento, incluyendo, al menos, la identificación de quién lo otorgó, cuándo y cómo se obtuvo, así como la versión de la cláusula informativa aplicable en dicho momento

- Gestión multicanal.

Proporcionar soporte para la obtención y gestión del consentimiento a través de distintos canales, incluyendo entornos digitales y presenciales, garantizando la coherencia de la información en todos ellos.

Los consentimientos deberán propagarse a los sistemas consumidores dentro de un plazo máximo definido mediante acuerdos de nivel de servicio (SLA) internos. La solución incluirá una cola persistente de eventos que garantice la entrega en caso de indisponibilidad temporal de los sistemas receptores.

El adjudicatario deberá proponer, como parte de su diseño técnico, los valores objetivo de dichos niveles de servicio, así como los mecanismos de monitorización y control asociados.

Asimismo, deberá definir los indicadores clave de operación del sistema, incluyendo, al menos, los tiempos de propagación, el ratio de errores en los procesos de sincronización, el nivel de disponibilidad del sistema y el grado de consistencia del dato entre los distintos sistemas integrados.

RQ. 5 - Gestión de tratamientos sin consentimiento

En aquellos tratamientos cuya base jurídica no sea el consentimiento —incluyendo, entre otros, los basados en obligación legal, ejecución de un contrato, misión en interés público o interés legítimo— no procederá la recogida ni la gestión de aceptación expresa por parte del interesado.

En estos supuestos, el sistema deberá garantizar la correcta información al interesado mediante la correspondiente cláusula informativa, así como su adecuado versionado. No obstante, no se generarán registros de consentimiento.

En su lugar, deberá registrarse la visualización efectiva de la cláusula informativa correspondiente.

Toda visualización de cláusula informativa deberá generar un identificador transaccional único, que sea exportable, trazable y apto para su utilización en procesos de auditoría en materia de RGPD.

RQ.6 – Registro y gestión de los consentimientos recogidos de manera manual

El modelo de gestión de tratamientos y consentimientos deberá ser multicanal. La circunstancia de que la recogida de datos o la manifestación de voluntad del interesado se produzca de manera presencial no exime de la obligación de su registro en el SCGTC.

Cuando la aceptación de un consentimiento o la formalización de un alta que implique tratamiento de datos personales se realice de forma presencial, el registro deberá efectuarse directamente en el SCGTC mediante un dispositivo conectado

(por ejemplo, tablet corporativa u otro terminal habilitado), mostrando en todo caso la versión vigente de la cláusula informativa correspondiente.

En estos supuestos, el sistema deberá registrar, como mínimo: la identificación del interesado, la identificación del empleado operador, la versión concreta de la cláusula mostrada, la fecha y hora del registro, así como la indicación expresa de que el canal de entrada ha sido presencial.

En aquellos casos en los que se realicen registros manuales, deberá quedar igualmente constancia del operador, la fecha, la hora y el canal de origen.

Toda recogida de consentimiento en soporte físico deberá ser digitalizada en un plazo máximo de 24 horas desde su obtención.

El uso de formularios en papel tendrá carácter excepcional y deberá estar debidamente justificado. En tales supuestos, será obligatoria su digitalización inmediata y su registro formal en el SCGTC, garantizando en todo caso la vinculación con la versión exacta de la cláusula informativa mostrada en el momento de la firma.

Los consentimientos recogidos en soporte físico deberán asociarse inequívocamente a la versión de la cláusula informativa vigente en el momento de su formalización.

Canales y experiencia de usuario

La interacción con el interesado deberá materializarse de forma coherente con el modelo de consentimiento y de cláusulas informativas previamente definido y gobernado. En este sentido, dicha interacción quedará condicionada a la existencia, validez y correcta versión de los elementos de gobierno del dato establecidos en el SCGTC.

RQ.7 – Área de preferencias (Front office)

En el momento de la recogida de datos personales, el interesado deberá recibir información clara, accesible y específica sobre el tratamiento que se vaya a realizar. Dicha información deberá incluir, como mínimo, la identidad del responsable del tratamiento, la finalidad del mismo, la base jurídica que lo legitima, los destinatarios previstos, los plazos de conservación y los derechos que asisten al interesado.

En consecuencia, toda interfaz o proceso que implique la recogida inicial de datos deberá incorporar la cláusula informativa correspondiente al tratamiento específico al que se encuentre vinculado.

En este ámbito deberán garantizarse, al menos, las siguientes funcionalidades:

- Consulta de tratamientos.

El usuario podrá consultar los tratamientos de datos personales que le resulten aplicables.

- Gestión de consentimientos.

El sistema permitirá la aceptación y revocación del consentimiento desde el área de usuario, cuando resulte procedente

- Transparencia de información.

Se deberá mostrar de forma clara la base jurídica, la finalidad del tratamiento y el estado del consentimiento o relación jurídica aplicable.

El área de preferencias deberá presentar de forma estructurada, accesible y comprensible la jerarquía de finalidades, sus bases jurídicas asociadas y las dependencias existentes entre tratamientos, garantizando la transparencia hacia el interesado.

Integración y eventos

El sistema deberá permitir su integración con el ecosistema corporativo del ICAM, actuando como repositorio maestro de información en materia de tratamientos y consentimientos, y habilitando la comunicación mediante eventos con los distintos sistemas corporativos.

RQ.8 – Integración con sistemas del ICAM

Partiendo de la premisa de que los sistemas satélite no actúan como autoridad de consentimiento, sino como sistemas consumidores del SCGTC, deberá garantizarse la integración del SCGTC con los distintos sistemas del ICAM, incluyendo, entre otros, Salesforce Marketing Cloud, Business Central, Tool Prive y cualquier otro sistema existente o que pueda implantarse en el futuro.

Asimismo, el SCGTC deberá integrarse con los sistemas legacy, así como con la web corporativa del ICAM.

En ningún caso los sistemas satélite podrán gestionar consentimientos de forma autónoma.

Se prohíben expresamente las integraciones punto a punto fuera de la plataforma Azure API Management. Toda integración deberá realizarse obligatoriamente a través de dicha capa, que actuará como punto único de control y gobierno de las comunicaciones.

El adjudicatario deberá definir un modelo de integración que garantice el desacoplamiento entre sistemas, la escalabilidad de la solución y la resiliencia de las comunicaciones, incluyendo mecanismos de gestión de errores, reintentos automáticos y control de consistencia de la información intercambiada. Dicho

modelo deberá ser homogéneo y aplicable a todos los sistemas integrados, incluidos los entornos legacy.

En el caso de integración con sistemas legacy, el adjudicatario deberá proporcionar adaptadores estándar, evitando en todo caso el desarrollo de integraciones ad hoc que comprometan la mantenibilidad y evolución del sistema.

RQ.9 – Eventos

- Eventos de cambio.

  Generación de eventos ante cambios relevantes en el sistema, incluyendo, al menos, altas, modificaciones y revocaciones.

- Webhooks.

  Notificación automática a los sistemas integrados mediante mecanismos de suscripción a eventos.

- Reintentos y resiliencia.

  Gestión de fallos en la comunicación, incluyendo mecanismos de reintento automático, control de entrega y estrategias de resiliencia en la emisión de notificaciones.

El adjudicatario deberá entregar un **Catálogo de Eventos**, que incluya, como mínimo, la definición de códigos de evento, estructuras de payload, niveles de prioridad, dependencias entre eventos y comportamiento ante errores o incidencias en la entrega.

Seguridad, auditoría y operación

Capa transversal del sistema que garantiza el control, el cumplimiento normativo y la continuidad operativa. Esta capa se soporta sobre los bloques funcionales previamente definidos y asegura su correcto funcionamiento conforme a los requisitos de riesgo, seguridad y normativa aplicable.

RQ.10 – Seguridad y cumplimiento

- Control de accesos.

  Gestión de roles y permisos basada en el principio de mínimo privilegio, garantizando el acceso únicamente a las funcionalidades y datos estrictamente necesarios según el perfil asignado.

- Auditoría.

  Registro inmutable de todas las operaciones relevantes del sistema. Las evidencias de auditoría deberán almacenarse en un repositorio segregado, sin

posibilidad de modificación por parte de perfiles operativos o técnicos, garantizando su integridad y trazabilidad.

- Cifrado.

Protección de los datos tanto en tránsito como en reposo, conforme a las políticas de seguridad corporativas.

- Privacidad por diseño.

Aplicación del principio de privacidad desde el diseño (*privacy by design*), asegurando que la protección de datos se incorpore de forma estructural en todas las fases del ciclo de vida del sistema.

- Cifrado.

El sistema deberá implementar cifrado en tránsito mediante protocolos seguros (TLS) y, cuando resulte aplicable, cifrado de datos en reposo conforme a las políticas corporativas de seguridad del ICAM.

RQ.11 – Evidencias y auditoría RGPD

- Registro de visualización. Registro de visualización de cláusulas cuando no hay consentimiento
- Evidencias completas. Almacenamiento de evidencias auditables.
- Exportación de evidencias. Capacidad de generar informes para auditorías.
- Sincronización horaria (NTP) y sellado de tiempo consistente en evidencias.

Toda exportación de datos deberá generar un identificador único de exportación, registrándose, como mínimo, la fecha, el responsable de la operación y el propósito de la misma.

RQ.12 – Rendimiento y escalabilidad

- Escalabilidad.

Deberá estar diseñado para soportar múltiples sistemas integrados y un alto volumen de operaciones, garantizando su rendimiento en escenarios de crecimiento..

- Disponibilidad.

Deberá garantizar un nivel de alta disponibilidad, asegurando la continuidad del servicio conforme a los objetivos definidos.

Se deberán definir KPIs obligatorios como: tiempo medio de propagación, disponibilidad, ratio de errores en eventos, y porcentaje de consentimientos pendientes de sincronización

3.2 Sede electrónica de Notificaciones y Comunicaciones

A continuación, se detalla a nivel funcional el proceso de notificaciones del ICAM, definiendo su operativa, los requisitos asociados y los elementos necesarios para garantizar su correcta gestión dentro del sistema.

Toda interacción del destinatario con las notificaciones se realizará a través de la sede electrónica del ICAM, con independencia del canal de envío utilizado. La sede electrónica constituirá el punto único de acceso para la consulta, gestión y visualización del contenido de las notificaciones, así como para la realización de cualquier actuación asociada por parte del usuario.

En este contexto, resulta necesario diferenciar entre notificaciones y comunicaciones, dado que ambos tipos de envío presentan naturaleza, implicaciones jurídicas y requisitos de gestión diferenciados.

Las **notificaciones** se definen como envíos de carácter formal emitidos por el ICAM que producen efectos administrativos o jurídicos sobre el destinatario. Este tipo de envíos deberá gestionarse mediante un sistema que garantice la identificación del destinatario, la puesta a disposición del contenido y la generación de evidencias que acrediten la correcta realización del acto de notificación, así como su trazabilidad completa a lo largo del proceso.

Las notificaciones podrán realizarse tanto por medios electrónicos, a través de la sede electrónica del ICAM, como mediante soporte papel a través de servicios de correo postal integrados.

Las **comunicaciones** se definen como envíos de carácter informativo destinados a trasladar información relevante a los usuarios del ICAM, sin que produzcan efectos administrativos o jurídicos directos. A diferencia de las notificaciones, no requerirán comparecencia electrónica para el acceso a su contenido.

El sistema deberá permitir que las comunicaciones estén disponibles en la sede electrónica mediante un listado de envíos, desde el cual el usuario podrá acceder a su contenido y consultar la documentación asociada. El sistema podrá registrar dicha consulta a efectos de gestión interna, sin que ello tenga implicaciones jurídicas.

Asimismo, las comunicaciones podrán realizarse tanto de forma individual como masiva, en función del público objetivo definido por la unidad emisora, y no estarán sujetas a plazos de caducidad para su consulta. Este tipo de envíos se utilizará principalmente para la

difusión de información institucional, avisos, recordatorios u otros contenidos de carácter informativo.

Una vez establecida esta diferenciación, el presente documento desarrolla de manera exclusiva el flujo funcional asociado a las notificaciones, dado que constituyen los envíos que requieren un mayor nivel de control, trazabilidad y generación de evidencias debido a sus implicaciones jurídicas y administrativas.

En consecuencia, los apartados siguientes describen el ciclo de vida, los requisitos y la operativa del sistema centrados en la gestión de notificaciones.

Actores del ciclo de vida de las notificaciones

Los actores que intervienen en el ciclo de vida de una notificación serán los siguientes:

Emisores:

Los organismos emisores corresponden a las distintas unidades o departamentos del ICAM responsables de generar y remitir notificaciones a los usuarios del Colegio. Entre ellos se incluyen, entre otros, el Servicio de Atención al Colegiado, Turno de Oficio, Formación, Comunicación y Marketing, así como otras áreas administrativas. Cada unidad emisora podrá dirigir sus envíos tanto a usuarios individuales como a colectivos determinados, en función del ámbito de actuación o del procedimiento correspondiente.

Destinatarios:

El destinatario es el usuario al que va dirigida la notificación. Podrá tratarse de personas colegiadas (ejercientes o no ejercientes), usuarios registrados en el portal del ICAM, representantes autorizados o entidades vinculadas. El acceso al contenido de los envíos se realizará a través de la sede electrónica del ICAM o del área reservada, previa autenticación del usuario.

Administradores:

Los administradores del sistema serán usuarios internos del ICAM responsables de la gestión y supervisión del sistema de notificaciones, incluyendo el control de los envíos realizados, la consulta del estado de las notificaciones y la gestión de incidencias asociadas al funcionamiento del sistema.

3.2.1 REQUERIMIENTOS

RQ.0 - Punto único de acceso

El sistema deberá disponer de una sede electrónica desde la cual el usuario pueda acceder y consultar todas las notificaciones y comunicaciones emitidas por el ICAM.

Este espacio actuará como punto único de acceso a los envíos electrónicos dirigidos al usuario, permitiendo la visualización, al menos, de las notificaciones pendientes de acceso, las notificaciones ya consultadas, las comunicaciones recibidas y el histórico completo de envíos.

RQ.1 - Acceso al sistema

El acceso al sistema de notificaciones se realizará exclusivamente a través de la sede electrónica, mediante los mecanismos de autenticación habilitados por el Colegio.

En todo momento deberá garantizarse un acceso seguro a la información y a los envíos disponibles para el usuario, conforme a los estándares de seguridad definidos por el ICAM.

RQ.2 – Ciclo de vida de una Notificación

GENERACIÓN

La generación de la notificación será realizada por la unidad correspondiente del ICAM, debiendo definirse, al menos, los siguientes elementos: destinatario o conjunto de destinatarios (envíos individuales o masivos), asunto o concepto, contenido del mensaje, documentación asociada, canal de envío (electrónico y/o postal) y, en su caso, el plazo máximo de acceso.

El sistema deberá permitir la generación de los documentos asociados mediante distintos mecanismos (plantillas, documentos estructurados, generación dinámica, adjuntos, entre otros), así como su visualización en diferentes formatos dentro de la sede electrónica.

PUESTA A DISPOSICIÓN / ENVÍO

En el caso de notificaciones electrónicas, el sistema deberá poner la notificación a disposición del destinatario en su área reservada dentro de la sede electrónica del ICAM, registrando de forma automática la fecha y hora exacta de disponibilidad.

En el caso de notificaciones en soporte papel, el sistema deberá permitir la integración con servicios de correo postal (como NEXEA), facilitando la generación del envío, su gestión y seguimiento, así como la incorporación de evidencias de entrega cuando estas estén disponibles.

El sistema deberá permitir la gestión combinada de ambos canales cuando resulte necesario.

El envío de notificaciones deberán poder hacerse via OTP o similar para el caso de usuarios no registrados en el sistema.

AVISO AL DESTINATARIO

El sistema podrá emitir avisos informativos al destinatario sobre la disponibilidad de una notificación mediante distintos canales (correo electrónico, sms, push, OTP u otros medios habilitados), sin que dichos avisos tengan carácter de notificación formal.

COMPARECENCIA ELECTRÓNICA Y ACCESO

El acceso del destinatario al contenido de la notificación implicará la realización de la comparecencia electrónica.

El sistema deberá registrar de forma automática la fecha y hora de acceso, generando un acuse de recibo o justificante electrónico asociado a la notificación.

Cuando resulte aplicable, dicho justificante deberá incorporar un sello de tiempo que garantice la integridad del documento y la acreditación fehaciente del momento de acceso.

GESTIÓN DEL PLAZO DE ACCESO

El sistema deberá permitir la definición de un plazo máximo de acceso a la notificación.

En caso de no producirse el acceso dentro del plazo establecido, el sistema deberá registrar esta circunstancia como parte de la trazabilidad del proceso, sin necesidad de gestionar estados explícitos de la notificación.

CONSULTA DE NOTIFICACIONES

El sistema deberá permitir al destinatario consultar sus notificaciones desde la sede electrónica, accediendo tanto al listado de envíos como al detalle de cada uno de ellos.

Cada notificación deberá incluir, al menos, la siguiente información: identificador, unidad emisora, asunto, fechas relevantes (puesta a disposición y acceso, en su caso), documentos asociados y justificante de recepción cuando exista.

TRAZABILIDAD Y REGISTRO DE EVIDENCIAS

El sistema deberá garantizar la trazabilidad completa del ciclo de vida de la notificación mediante el registro de todos los eventos relevantes, incluyendo, entre otros: generación, puesta a disposición, accesos, generación de justificantes, envíos postales y evidencias de entrega.

Dicha información deberá almacenarse de forma estructurada, con garantías de integridad e inalterabilidad, y estar disponible para su consulta por parte de usuarios autorizados, permitiendo la auditoría, control y acreditación completa del proceso.

RQ.3 - Aceptación y firma previa a la lectura

El sistema deberá permitir la parametrización de determinadas notificaciones que requieran, con carácter previo al acceso a su contenido, la aceptación expresa y, en su caso, la firma electrónica por parte del destinatario.

Esta funcionalidad deberá ser configurable en función del tipo de proceso o procedimiento asociado a la notificación, siendo el ICAM quien determine en cada caso qué notificaciones quedan sujetas a este requisito.

En estos supuestos:

- El usuario no podrá acceder al contenido de la notificación sin haber realizado previamente la aceptación y/o firma requerida.
- El sistema deberá registrar la evidencia de la aceptación y/o firma, incluyendo fecha, hora y mecanismo utilizado.
- La aceptación o firma deberá formar parte de la trazabilidad completa de la notificación.

RQ.4 – Gestión de documentos asociados

El sistema deberá permitir asociar a cada notificación uno o varios documentos, incluyendo el documento principal, anexos, justificantes y cualquier otro contenido relevante.

Asimismo, deberá permitir múltiples formas de visualización de dichos documentos (visualización en línea en la sede electrónica, descarga en distintos formatos, acceso estructurado, entre otros), garantizando la accesibilidad y comprensión por parte del usuario.

RQ.5 – Posibilidad de Integración con servicios de terceros para generación de evidencias

El sistema deberá permitir la integración con servicios externos especializados en la generación de evidencias electrónicas de comunicaciones y notificaciones, tales como la plataforma de Lleida.net, mediante el uso de APIs.

En particular, deberá contemplarse la utilización de servicios de certificación de envío, contenido y entrega de notificaciones electrónicas, que permitan la obtención de evidencias fehacientes y verificables.

RQ.6 – Histórico unificado de notificaciones

La sede electrónica deberá disponer de un histórico completo de todas las notificaciones recibidas por el usuario, accesible desde su área personal.

Este histórico deberá incluir la totalidad de las notificaciones, con independencia del canal de envío utilizado (electrónico o postal) o del mecanismo de generación.

Cada registro deberá permitir la consulta, al menos, de:

- Datos identificativos de la notificación
- Estado
- Fechas relevantes
- Documentación asociada
- Evidencias generadas

Este histórico actuará como repositorio único de consulta para el usuario, garantizando la centralización, trazabilidad y accesibilidad de todas las notificaciones recibidas.

RQ.7 – Generación automática de Notificaciones

El sistema deberá permitir la generación automática de notificaciones a partir de reglas de negocio o procesos previamente definidos en el sistema.

Asimismo, deberá permitir la configuración flexible del contenido de las notificaciones generadas automáticamente, incluyendo el uso de plantillas predefinidas y la incorporación de campos de texto libre, permitiendo su adaptación a distintos contextos y necesidades operativas de las unidades emisoras.

RQ.8 – Registro y Trazabilidad

El sistema deberá mantener un registro completo de todas las actuaciones realizadas sobre cada notificación.

Este registro deberá incluir, al menos, la fecha de emisión, la fecha de puesta a disposición, los accesos realizados por el usuario, la aceptación o rechazo de la notificación y, en su caso, la fecha de expiración.

Dicha información deberá conservarse de forma estructurada, garantizando su integridad, y estar disponible para su consulta por parte de los administradores del sistema, permitiendo la auditoría y supervisión completa del proceso de notificación.

4. ARQUITECTURA

Con el objetivo de garantizar que la solución propuesta sea integral y transversal a toda la arquitectura actualmente en proceso de implantación, se incluye (a modo referencial) la arquitectura vigente. **Esta se basa en un *stack* tecnológico sustentado en soluciones Microsoft, microservicios backend en Java, frontales en angular y contempla, con una visión de futuro, las implementaciones previstas en modalidad SaaS**, así como su relación con la arquitectura *On-Premises.*

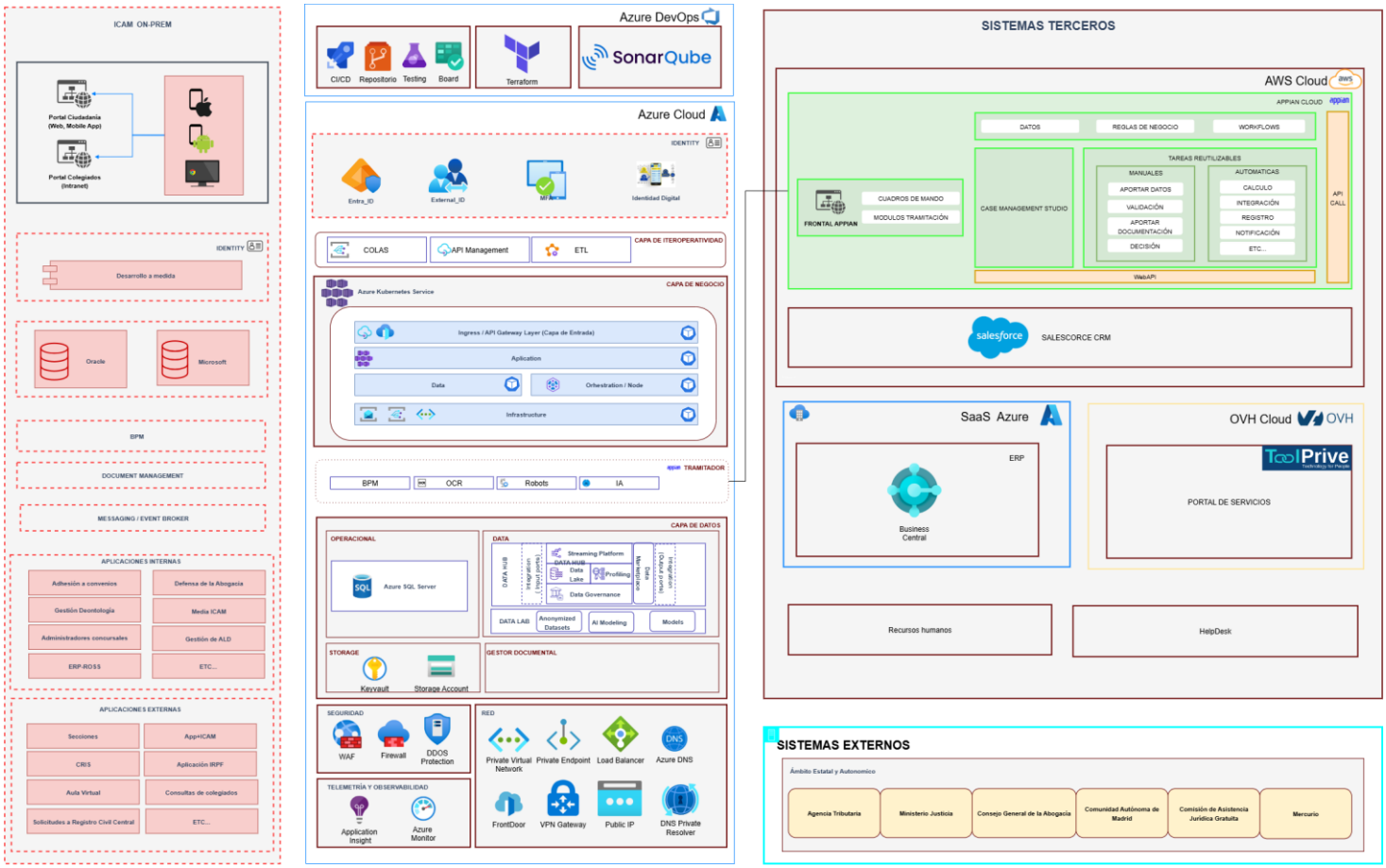

Ilustración 1 - Arquitectura To Be

Debe tenerse en cuenta que el esquema de arquitectura aquí representado se encuentra en proceso de evolución y se actualiza de manera continua, conforme se adoptan decisiones definitivas sobre las tecnologías, servicios y/o aplicaciones a incorporar.

Arquitectura Futura

La visión arquitectónica futura plantea una evolución hacia un **modelo híbrido**, en el cual las capacidades existentes se complementen con **soluciones SaaS y en la nube**, fortaleciendo la seguridad, la escalabilidad y la disponibilidad del sistema del ICAM.

La arquitectura final deberá incluir escenarios de resiliencia, fallos parciales y un diagrama que muestre claramente qué componente es autoridad del dato en cada etapa.

4.1 Objetivo técnico

4.1.1 Proceso RGPD

El objetivo técnico del presente proyecto es la **definición, diseño e implantación de un Sistema Centralizado de Gestión de Tratamientos y Consentimientos (SCGTC)** que permita la gestión integral, estructurada, trazable y conforme a la normativa vigente de los tratamientos de datos personales, sus bases jurídicas, las cláusulas informativas y los consentimientos asociados, **actuando como repositorio maestro corporativo y fuente única, consistente y confiable de referencia dentro del ecosistema tecnológico existente**.

La solución deberá integrarse con la arquitectura actual, en la que Appian constituye la plataforma central sobre AWS para la gestión de procesos, datos, reglas de negocio y capacidades de front office (cuadros de mando, módulos de tramitación y portal de usuario), siendo esta la base sobre la que deberán implementarse los flujos de gestión, los modelos de datos, la lógica de negocio y los circuitos de aprobación asociados al **gobierno de tratamientos, cláusulas y consentimientos**. Asimismo, deberá interoperar con los componentes de integración expuestos en Azure, incluyendo API Management y bases de datos corporativas.

El diseño técnico deberá ser propuesto por el adjudicatario, contemplando una arquitectura interoperable, escalable y multicanal que utilice Appian como núcleo de orquestación de procesos, garantizando que toda la lógica de backend, gestión de workflows, control de estados, versionado y aprobaciones se implementa sobre dicha plataforma, mientras que el resto de componentes tecnológicos se integrarán de forma desacoplada para la exposición de servicios, la sincronización de información y la gestión de eventos, asegurando la trazabilidad completa, el control de accesos, la auditoría y la sostenibilidad de la solución en el medio y largo plazo.

La solución deberá permitir auditorías cruzadas entre SCGTC, RAT y sistemas consumidores, garantizando la coherencia del dato en todo el ecosistema. A estos efectos, el adjudicatario deberá definir en su propuesta el modelo de autoridad del dato por dominio funcional, identificando de forma explícita qué sistemas actúan como fuente de referencia en cada caso, así como los mecanismos de sincronización, control y resolución de discrepancias entre ellos.

4.1.2 Sede electrónica de Notificaciones y Comunicaciones

El objetivo técnico del presente proyecto es la definición, **diseño e implantación de un Sistema Centralizado de Gestión de Notificaciones y Comunicaciones Electrónicas**, que permita la gestión integral, trazable y segura del ciclo de vida de los envíos dirigidos a los usuarios del ICAM, actuando como plataforma corporativa única para la generación, distribución, consulta y seguimiento de notificaciones y comunicaciones.

La solución deberá integrarse con la arquitectura tecnológica existente, permitiendo la implementación de los flujos de generación, puesta a disposición, comparecencia, gestión de estados y control de plazos asociados a las notificaciones, así como la gestión diferenciada de comunicaciones informativas.

El sistema deberá contemplar una arquitectura interoperable, escalable y multicanal, que permita:

- La integración con sistemas corporativos emisores de notificaciones.
- La interoperabilidad con servicios externos (correo electrónico, servicios postales, etc.) mediante microservicios independientes a traves del API Management.
- La exposición de servicios mediante APIs gestionadas a través de los componentes de integración corporativos.

Asimismo, deberá garantizar la trazabilidad completa del proceso, mediante el registro de eventos relevantes (emisión, puesta a disposición, accesos, comparecencia, generación de evidencias, expiraciones, etc.), así como el control de accesos, la auditoría y la disponibilidad de la información para su consulta por usuarios autorizados.

La solución deberá diseñarse bajo principios de seguridad, privacidad y cumplimiento normativo, asegurando la confidencialidad, integridad y disponibilidad de la información, así como la correcta gestión de evidencias electrónicas asociadas a las notificaciones con efectos jurídicos.

Finalmente, el diseño técnico deberá asegurar la sostenibilidad, mantenibilidad y evolución del sistema en el medio y largo plazo, mediante una arquitectura desacoplada basada en microservicios, alineada con las directrices tecnológicas del ICAM.

4.2 Entregables

Entregable	Apartados	Descripción	Formato
Propuesta Técnica Estandarizada de Solución	Definición y análisis de alternativas de solución	Evaluación comparativa de posibles soluciones tecnológicas o funcionales, con análisis de ventajas, desventajas y recomendación final. **Máx: 4.000 caracteres**	Documento
	Diseño de la solución	Diseño detallado de la arquitectura, componentes y procesos de la solución recomendada, incluyendo diagramas, flujos y dependencia. **Máx: 6.000 caracteres**	
	Referencias	Listado de referencias de procesos iguales o similares a los descritos en este pliego, donde se evidencie la experiencia del proveedor en implementación de procesos de este tipo. **Máx: 3.000 caracteres**	
	Listado de aceleradores	Identificación de componentes reutilizables, frameworks o herramientas (aceleradores) que permitan minimizar tiempos y aumentar la calidad del desarrollo. **Máx: 2.500 caracteres**	
	Plan de proyecto	Se debe definir un plan de proyecto en donde se refleje fases, duración estimada, hitos clave y entregables parciales. **Máx: 3.500 caracteres**	
	Enfoque metodológico	Describir la metodología a aplicar en la ejecución, gestión de riesgos y control de calidad. **Máx: 3.000 caracteres**	
	Equipo de Trabajo	Listado del equipo de trabajo. **Máx: 2.000 caracteres**	
	Plan de pruebas	Casos de prueba y ejecución. **Máx: 3.000 caracteres**	

4.3 Requisitos mínimos de seguridad aplicables a desarrollo

Las actuaciones incluidas en este objeto deberán ejecutarse conforme a las buenas prácticas en materia de ciberseguridad, protección de datos y desarrollo de software, asegurando la continuidad operativa del sistema y la no alteración de los servicios actualmente en producción.

El equipo de Seguridad de la Información y Calidad del ICAM ha definido los siguientes criterios de **Desarrollo Seguro de Software**, cuyo cumplimiento debe garantizar el proveedor

- **Revisión estática de código:** con herramientas como SonarQube. Umbral mínimo recomendado: 80% de cobertura de código.
- **Gestión de dependencias seguras:** revisión de librerías, uso de repositorios oficiales y control de versiones.
- **Pruebas automatizadas:** unitarias, de integración y funcionales.
- **Análisis de vulnerabilidades:** antes del paso a producción, con reporte y corrección de CVEs críticos o altos.
- **Evidencias esperadas:**
    - Informe SonarQube.
    - Resultados de pruebas automatizadas.
    - Informe de revisión de seguridad del código.

Adicionalmente, se encuentra disponible el Anexo 1. Cláusula de Desarrollo Seguro en Entornos Cloud y Plataformas Integradas del ICAM, donde se detallan todas y cada una de las cláusulas que el proveedor debe cumplir.

a) PLAN DE GARANTÍA Y SOPORTE

El proveedor seleccionado deberá proporcionar un **Plan de Garantía y Soporte Post-Implantación** que asegure la correcta operación, estabilidad y continuidad del sistema durante el periodo posterior a la aceptación formal del proyecto.

1. Periodo de garantía

El periodo mínimo será de seis (6) meses naturales a partir de la aceptación del proyecto. Durante este plazo, el proveedor seleccionado deberá:

- Corregir, sin coste adicional, los defectos o incidencias derivadas del desarrollo, integración o configuración.
- Garantizar la disponibilidad y el correcto funcionamiento de la solución en los entornos productivos del ICAM.
- Mantener la compatibilidad e interoperabilidad con los servicios y sistemas existentes.

Durante la garantía, el adjudicatario deberá monitorizar de forma continua las colas de eventos, SLAs de propagación e integridad del dato, remitiendo informes mensuales al ICAM:

2. Alcance del soporte

El soporte técnico comprenderá:

- Soporte correctivo: resolución de errores o anomalías funcionales.
- Soporte evolutivo menor: ajustes derivados de cambios normativos, de seguridad o de integración.
- Asistencia funcional básica: apoyo remoto para la configuración y el uso del sistema.
- Todas las incidencias deberán registrarse en la herramienta o canal de comunicación establecido por el ICAM.

3. Niveles de servicio

Durante el periodo de garantía se aplicarán los **Acuerdos de Nivel de Servicio (ANS)** definidos en el presente pliego, manteniendo los mismos tiempos de respuesta y resolución establecidos para la fase de ejecución.

4. Procedimiento de atención

El proveedor seleccionado deberá disponer de un equipo de soporte técnico con conocimiento del proyecto, que prestará atención en horario laboral, de lunes a viernes de 9:00 a 18:00 horas, a través de los canales de comunicación definidos por el ICAM.

Cada incidencia deberá documentarse, indicando su nivel de criticidad y las medidas adoptadas para su resolución.

5. Cierre del periodo de garantía

Al finalizar el periodo de garantía, el proveedor seleccionado deberá presentar un **informe de cierre**, que incluirá el detalle de las incidencias atendidas, el cumplimiento de los ANS y las recomendaciones técnicas para la continuidad del servicio.

La validación de este informe por parte del ICAM será condición necesaria para la aceptación definitiva del proyecto y para el cierre administrativo del contrato.

5. MODELO DE SEGUIMIENTO

a) PLANIFICACIÓN Y DIRECCIÓN DE LOS TRABAJOS

El equipo de trabajo que el proveedor seleccionado aporte para dar cumplimiento al objeto del contrato deberá colaborar con otros equipos del ICAM y de la OTD.

La planificación deberá establecer, de manera clara y concreta, cada uno de los hitos en los que se distribuye el proyecto, especificando las fechas de inicio y fin, así como las actividades y tareas que deben realizarse y los entregables asociados.

b) MODELO DE RELACIÓN

Entre las reuniones que deben tener lugar se encuentran las siguientes:

- Comité de Seguimiento Operativo:
  - **Periodicidad**: semanal.
  - **Participantes**: gestores de proyectos del ICAM, el jefe de proyecto y los gestores de proyectos de la OTD, así como el jefe de proyecto del proveedor.

- Reuniones de Coordinación entre el proveedor y la OTD:
  - **Periodicidad**: semanal, pudiendo establecerse una frecuencia mayor en función de las necesidades.
  - **Participantes**: el jefe de proyecto y los gestores de proyectos de la OTD, junto con el jefe de proyecto del proveedor.

c) APROBACIÓN DE LOS ENTREGABLES

Los entregables se considerarán aprobados únicamente cuando el Gestor de Proyectos del ICAM, en conjunto con el jefe de proyecto y los Gestores de Proyectos de la OTD, hayan validado formalmente su completitud y conformidad, de acuerdo con lo establecido en la propuesta técnica presentada por el proveedor.

Dicha validación constituirá la aceptación oficial del entregable para todos los efectos.

d) PROPIEDAD INTELECTUAL

Según la legislación vigente en materia de propiedad intelectual y de protección jurídica de los programas de ordenador, el proveedor seleccionado acepta expresamente que la propiedad de todos los productos (tanto software en cualquier forma o soporte, así como datos y/o información, incluida la documentación preparatoria, especificaciones,

presentaciones, DLL, scripts, etc.) que sean elaborados por el proveedor seleccionado en ejecución del Contrato, y, en particular, todos los derechos de propiedad intelectual y/o industrial que deriven de los mismos, corresponderá únicamente al ICAM, con exclusividad y sin más limitaciones que las que imponga el ordenamiento jurídico.

A los efectos previstos en el párrafo anterior, el proveedor seleccionado se compromete a entregar al ICAM toda la documentación técnica, así como los trabajos y materiales generados en los procesos de análisis, diseño, desarrollo, implantación, mantenimiento y realización de pruebas. Toda esta documentación quedará en poder del ICAM a la finalización del Contrato, sin que el proveedor seleccionado pueda conservarla, obtener copia de esta, utilizarla o facilitarla a terceros sin la expresa autorización del ICAM, la cual podrá otorgarse, en su caso, previa petición formal del proveedor seleccionado en la que se indique el fin para el que se solicita.

El proveedor seleccionado cede de manera exclusiva al ICAM todos los derechos necesarios, sin que ello genere derecho alguno para el proveedor de dichos programas, a fin de que el ICAM pueda realizar copias de estos, instalarlos en cuantos ordenadores, dispositivos móviles y demás equipos informáticos estime oportuno, y utilizarlos en el ejercicio de su actividad. Asimismo, el ICAM podrá modificar el código fuente con el fin de adaptarlo a sus características o necesidades específicas y/o ponerlo a disposición de terceros y, en general, ceder a terceros, ya sea mediante licencias propietarias, libres o abiertas, los derechos que deba ostentar sobre el objeto del contrato.

Esta cesión se extiende a cualquier derecho de explotación, en cualquier modalidad y bajo cualquier formato, por todo el periodo de duración máxima de los derechos y para todo el mundo, sin perjuicio de los derechos de terceros sobre componentes integrados.

e) ENTREGABLES Y DOCUMENTACIÓN DEL SERVICIO

Como parte de los trabajos objeto del contrato, el proveedor seleccionado se compromete a generar y facilitar toda la documentación de soporte y las actuaciones técnicas, así como a ponerla a disposición de forma continuada y actualizada en un repositorio de información accesible por el ICAM.

Toda la documentación quedará en propiedad exclusiva del ICAM, sin que el proveedor seleccionado pueda conservarla, obtener copia de esta ni facilitarla a terceros sin la expresa autorización formal del ICAM.

6. EQUIPO DE TRABAJO

El equipo de trabajo requerido para la ejecución del objeto del presente documento será propuesto por el proveedor, quien se compromete a detallar, de manera exhaustiva, los siguientes aspectos relacionados con los miembros que conformarán el equipo asignado a la prestación de los servicios:

1. **Perfiles de los miembros del equipo:** El proveedor deberá identificar y proponer los perfiles profesionales adecuados para cada función dentro del equipo de trabajo, especificando las competencias técnicas y habilidades necesarias para cumplir con los requisitos del contrato.
2. **Responsabilidades:** Se deberán definir claramente las responsabilidades y tareas específicas que asumirá cada miembro del equipo en relación con los objetivos y actividades que conforman el alcance del proyecto. Esto incluye la descripción detallada de las funciones y actividades de las cuales será responsable el equipo durante el desarrollo del proyecto.
3. **Titulación académica:** El proveedor deberá acreditar la titulación académica de cada miembro del equipo, asegurándose de que dicha formación sea pertinente y adecuada para el desempeño de las tareas asignadas. En todos los casos, será obligatorio presentar documentación oficial que respalde la formación académica de los profesionales propuestos.
4. **Experiencia profesional:** Se deberá presentar un historial detallado de la experiencia profesional de cada miembro del equipo, destacando la experiencia relevante en proyectos de características similares al objeto del presente proyecto. Se especificarán los años de experiencia y los proyectos previos en los que haya participado cada profesional, con especial énfasis en aquellos que impliquen trabajos de naturaleza y complejidad comparables.
5. **Certificaciones:** El proveedor deberá garantizar que los miembros del equipo cuenten con las certificaciones necesarias, tanto generales como específicas, que acrediten su competencia técnica en las áreas relevantes del proyecto. Dichas certificaciones deberán ser válidas y estar emitidas por entidades competentes y reconocidas en el sector, conforme a las exigencias del proyecto.
6. **Herramientas y tecnologías:** El proveedor deberá detallar las herramientas y tecnologías que el equipo utilizará para la ejecución de las actividades del contrato. Este apartado incluirá software, plataformas, equipamiento especializado y cualquier otro recurso técnico necesario para garantizar la correcta ejecución del trabajo.

7. **Cantidad (FTE):** El proveedor deberá detallar la cantidad de FTE (Full-Time Equivalente) asociada a cada perfil propuesto.

En caso de que alguno de los miembros inicialmente propuestos sea reemplazado durante la ejecución del proyecto, el proveedor se compromete a presentar al contratante, para su aprobación, un sustituto que posea cualificaciones y experiencia iguales o superiores a las del profesional reemplazado, garantizando en todo momento la continuidad y la calidad del servicio.

El equipo de trabajo descrito será considerado un componente esencial para el cumplimiento de los términos y objetivos establecidos en el presente proyecto. La adecuada selección y evaluación de cada uno de los miembros será fundamental para asegurar el éxito del proyecto y la satisfacción de los requisitos del ICAM.

7. CRITERIOS DE VALORACIÓN

Cada uno de los criterios de valoración se puntuará conforme a la puntuación de referencia, obtenida mediante la ponderación entre el peso asignado al criterio y su valor ponderado.

La valoración tendrá como objetivo identificar la propuesta que mejor se alinee con las necesidades del ICAM para la ejecución del proyecto "RGPD y Notificaciones", garantizando la coherencia funcional, técnica y arquitectónica de la solución propuesta.

Si el proveedor considera, en base a su experiencia, que la propuesta puede dividirse en fases diferentes y define su alcance, se valorará tanto su propuesta como la justificación presentada.

Tipología	Fase	Descripción
Servicios	RGPD y Notificaciones	Desarrollo e implementación de Sistema Centralizado de Gestión de Tratamientos y Consentimientos. Definición, diseño e implantación de un Sistema Centralizado de Gestión de Notificaciones y Comunicaciones Electrónicas

Los aspectos para considerar son los siguientes:

Criterios	Peso	Puntos	Ponderado
Precio	60%	60	3
Calidad Técnica de la Propuesta	30%	30	1,5
Mejoras voluntarias	5%	5	0,25
Aspectos sociales y medioambientales	5%	5	0,25
Totales	100%	100	5

a) CRITERIOS CUALITATIVOS

Los criterios no económicos (calidad técnica, mejoras voluntarias y aspectos sociales y medioambientales) se evaluarán de forma cualitativa, con base en:

- La documentación técnica presentada por cada proveedor.
- Las evidencias, referencias o certificaciones aportadas.

- El grado de cumplimiento de los requisitos establecidos.

b) CRITERIOS DE EVALUACIÓN TÉCNICOS

El proceso de evaluación técnica se fundamentará en la documentación presentada por los licitadores y en las evidencias que acrediten el cumplimiento de los requisitos establecidos. Los criterios técnicos no económicos se valorarán de forma cualitativa, conforme a lo indicado en este pliego, garantizando la objetividad y la trazabilidad del proceso.

Criterio Técnico	Descripción conforme al pliego	Forma de evaluación
Calidad técnica de la propuesta	Se valorará el grado de cumplimiento de los requisitos técnicos establecidos, la adecuación de la solución a la arquitectura definida y la alineación con los estándares de desarrollo seguro indicados en el documento y sus anexos.	Evaluación cualitativa según la documentación técnica presentada por el licitador.
Metodología y planificación de los trabajos	Se considerará la claridad y concreción en la planificación, incluyendo fases, hitos, actividades y entregables conforme al modelo de seguimiento descrito.	Revisión documental de la planificación y coherencia con los hitos definidos.
Equipo de trabajo propuesto	Se analizarán los perfiles profesionales, titulaciones, experiencia y certificaciones presentadas, de acuerdo con las exigencias establecidas en el apartado "Equipo de Trabajo".	Evaluación documental y verificación del cumplimiento de los requisitos de perfil y experiencia.
Cumplimiento de requisitos de seguridad	Se comprobará la aplicación de las buenas prácticas de ciberseguridad, revisión de código, gestión de dependencias y pruebas automatizadas conforme al apartado "Requisitos mínimos de seguridad aplicables a desarrollo".	Evaluación binaria (cumple/no cumple) mediante verificación documental.
Evidencias y documentación técnica	Se valorarán las evidencias, referencias o certificaciones aportadas que acrediten la conformidad con los requisitos del pliego.	Evaluación cualitativa basada en la documentación entregada.

c) PRECIO

La puntuación correspondiente al criterio de precio se obtendrá aplicando la fórmula siguiente:

> **Puntuación = (Oferta de menor importe / Oferta evaluada) × Puntuación máxima del criterio.**

La oferta económica de menor importe recibirá la puntuación máxima, mientras que las restantes ofertas serán valoradas de manera proporcional.

8. ANEXOS

ANEXO 1. CLÁUSULA DE DESARROLLO SEGURO EN ENTORNOS CLOUD Y PLATAFORMAS INTEGRADAS DEL ICAM

El proveedor seleccionado deberá garantizar que toda actividad de desarrollo, integración o mantenimiento de aplicaciones y servicios alojados en plataformas Cloud corporativas (incluyendo Appian Cloud y Azure DevOps) **se realice dentro de los entornos y herramientas aprobadas por el ICAM**, **siguiendo los principios de seguridad y privacidad** desde el diseño y por defecto, conforme al ENS, ISO/IEC 27001:2022, la normativa vigente de protección de datos personales, así como las políticas, normativas y procedimientos de aplicación en el Colegio en materia de seguridad de la información y protección de datos.

1. Entorno y control de desarrollo

- Los desarrollos se realizarán en la plataforma Appian Cloud del ICAM, utilizando los entornos proporcionados por Appian (Desarrollo, Pruebas y Producción) y las herramientas corporativas de Azure DevOps para la gestión del ciclo de vida, control de versiones y despliegues automatizados.
- El proveedor seleccionado no podrá desplegar ni administrar infraestructuras externas distintas de Appian Cloud o Azure DevOps sin autorización expresa del ICAM.
- El proveedor seleccionado deberá aplicar un proceso documentado de gestión de vulnerabilidades y actualizaciones, garantizando la corrección de fallos de seguridad críticos dentro de los plazos definidos por el ICAM.
- Los accesos se realizarán mediante usuarios corporativos asignados por Azure AD, con autenticación multifactor (MFA) y roles limitados al proyecto.

2. Seguridad por diseño y ciclo de vida del software

- Los desarrollos deberán aplicar los principios de seguridad por defecto y mínimo privilegio, evitando configuraciones abiertas o credenciales embebidas.
- Todo el ciclo de vida del software seguirá el flujo corporativo de Azure DevOps (feature → develop → release → main).
- Los pipelines ejecutarán de forma automatizada las verificaciones de seguridad (Health Check, SAST, SCA, DAST), y los resultados se considerarán requisitos de aceptación obligatorios antes del paso a producción. Los resultados del Health Check y del Design Guidance deberán ser 'Healthy' o 'Acceptable' antes del despliegue.
- El proveedor seleccionado aplicará metodologías de desarrollo seguro reconocidas (p. ej., OWASP, Microsoft SDL), que garanticen la incorporación

sistemática de controles de seguridad desde la fase de diseño hasta la puesta en producción.

- El proveedor seleccionado deberá notificar inmediatamente al ICAM cualquier incidente o sospecha de incidente de seguridad detectado durante el ciclo de vida del desarrollo, conforme a las instrucciones previstas en el Contrato de Prestación de Servicios y, en su caso, en el correspondiente acuerdo de encargo del tratamiento.

3. Segregación de entornos y funciones

- Los entornos DEV, QA, PRE y PROD estarán separados física y lógicamente.
- El proveedor seleccionado no podrá promover código a producción; la aprobación corresponderá al área de Tecnología del ICAM.
- Todas las operaciones quedarán trazadas y registradas en los logs de Azure DevOps y Appian.

4. Control de acceso y autenticación

- Los accesos a Appian Cloud se integrarán con el sistema de identidad corporativo (Azure Active Directory) mediante SSO SAML/OIDC y autenticación multifactor (MFA). Las soluciones deberán seguir los mecanismos corporativos de SSO y MFA, y los roles y permisos en Appian se definirán conforme al principio de mínimo privilegio y se revisarán periódicamente.
- Los roles y permisos en Appian se definirán siguiendo el principio de mínimo privilegio y se revisarán periódicamente.

5. Privacidad desde el diseño y por defecto

- Para garantizar la protección de datos personales y los derechos y libertades de las personas físicas, desde las fases de diseño, desarrollo, pruebas, implementación y mantenimiento de cualquier proyecto que afecte a datos personales responsabilidad del ICAM, o a datos personales que el ICAM trate en su calidad de encargado del tratamiento, el proveedor seleccionado se compromete a integrar todas las garantías necesarias para cumplir con los principios de privacidad desde el diseño y por defecto.
- El proveedor seleccionado tiene prohibido el uso de datos reales en entornos no productivos.
- El proveedor seleccionado deberá colaborar activamente con el ICAM en el proceso de privacidad desde el diseño y por defecto, incluyendo el análisis de riesgos para los derechos y libertades de las personas y, en su caso, la Evaluación de Impacto en la Protección de Datos que corresponda; así como en la adopción de medidas correctoras derivadas de dichos análisis y evaluaciones.

- En caso de subcontratar parte del desarrollo, el proveedor seleccionado garantiza que los subcontratistas asuman los mismos compromisos y obligaciones que los previstos para el proveedor seleccionado.

6. Integraciones y APIs

- Las integraciones entre Appian Cloud y los microservicios del ICAM se realizarán exclusivamente a través de Azure API Management, empleando los mecanismos de autenticación corporativos (OAuth 2.0, JWT, mTLS). Las conexiones desde la plataforma de desarrollo hacia Azure se establecerán mediante canal seguro (VPN IPSec o PrivateLink) aprobado por el ICAM. Cualquier uso de servicios o componentes de terceros (incluyendo subcontratistas o librerías externas) deberá contar con autorización previa y expresa del ICAM.
- Toda API desarrollada o consumida deberá ajustarse a las políticas de seguridad y autenticación corporativas configuradas en el Azure API Management del ICAM (OAuth2, JWT, mTLS).
- El proveedor seleccionado deberá utilizar las suscripciones, endpoints y certificados proporcionados por el ICAM, sin emplear tokens o credenciales propias.
- Cualquier integración estará sujeta a una revisión de seguridad obligatoria antes de su despliegue.

7. Validación y revisión de seguridad

- Previo a la liberación de cada versión, se ejecutarán los controles de:
- Appian Health Check Y Design Guidance (resultado “Healthy” o “Acceptable”).
- Análisis SAST/SCA/DAST integrados en los pipelines del ICAM.
- Pruebas funcionales y de rendimiento en entorno de PREPRODUCCIÓN.
- El proveedor seleccionado deberá subsanar todos los hallazgos críticos o altos antes de la aprobación final.

8. Trazabilidad y auditoría

- Todos los despliegues y pruebas deberán quedar registrados en Azure DevOps con logs, artefactos y aprobaciones electrónicas.
- El ICAM conservará las evidencias generadas como parte del expediente de seguridad.
- Los logs de auditoría y actividad de Appian Cloud se recogerán a través de las herramientas de administración de Appian y se integrarán, cuando sea posible, en el SIEM corporativo del ICAM. Los despliegues y pruebas quedarán igualmente registrados en Azure DevOps con logs, artefactos y aprobaciones electrónicas.

9. Evaluación y cumplimiento del proveedor

- El proveedor seleccionado deberá mantener vigentes las certificaciones aportadas y/o las medidas de seguridad y, en su caso, de protección de datos personales identificadas dentro del proceso de homologación y validadas por el ICAM.
- Anualmente, ICAM podrá exigir la realización de auditorías técnicas y/o solicitar evidencias documentales – incluyendo informes de auditoría – que acrediten el cumplimiento de los requisitos de seguridad de la información y, en su caso, de protección de datos personales establecidos.
- En caso de incidentes graves o cambios significativos, el proveedor seleccionado deberá notificar inmediatamente al ICAM.
- El incumplimiento de los requisitos de esta cláusula será considerado un incumplimiento grave de las condiciones de seguridad.

https://protecciondatos-lopd.com/empresas/compliance/software/

ANEXO 2. MICROSERVICIO DE NOTIFICACIONES

Este componente se encuentra ya implementado y operativo, ofreciendo funcionalidades relacionadas con la gestión de envíos de comunicaciones sujetas a procesos de firma electrónica, así como la consulta y seguimiento de su estado. A continuación se indica lo que hay implementado actualmente en el ICAM para que pueda ser utilizado y aprovechado para su incorporación en la solución global del sistema de notificaciones y comunicaciones del ICAM.

El microservicio actúa como capa de abstracción para la gestión de procesos de firma electrónica, encapsulando la integración con el proveedor externo (Lleida) y exponiendo una serie de endpoints REST que permiten iniciar procesos de firma, consultar su estado, obtener información detallada de los firmantes y recibir actualizaciones asíncronas del proveedor. Este enfoque permite desacoplar la lógica de negocio de los sistemas consumidores respecto a los detalles de integración con el proveedor de firma.

En concreto, el microservicio dispone de los siguientes endpoints:

- Start Signature, que permite el envío de una comunicación para su firma iniciando un nuevo proceso y generando un identificador único asociado.
- Get Signature Status, que permite obtener el estado global de un proceso de firma específico, indicando si se encuentra en curso, completado o en error
- Get Signatory Status, que facilita la consulta del estado individual de un firmante dentro del proceso
- Get Signature Details, que proporciona un mayor nivel de detalle sobre el estado de firma de un firmante concreto

- Callback, que permite la recepción de notificaciones asíncronas por parte del proveedor Lleida con los cambios de estado de los envíos realizados, asegurando así la actualización en tiempo real sin necesidad de consultas continuas.

A continuación, se incluyen los diagramas de flujo representativos del funcionamiento del microservicio, diferenciando entre el flujo general para las APIs de tipo "Start Signature" y el flujo general de Callback.

En el flujo general para las APIs de tipo "Start Signature", el sistema cliente realiza la llamada a cualquiera de los endpoints expuestos (Start Signature, Get Signature Status, Get Signatory Status o Get Signature Details). El microservicio recibe la petición, valida la solicitud y prepara la invocación al proveedor Lleida. A continuación, se realiza la llamada a la API correspondiente de Lleida, que procesa la solicitud y devuelve una respuesta. El microservicio procesa dicha respuesta y la transforma en un formato adecuado, devolviéndola finalmente al sistema cliente solicitante.

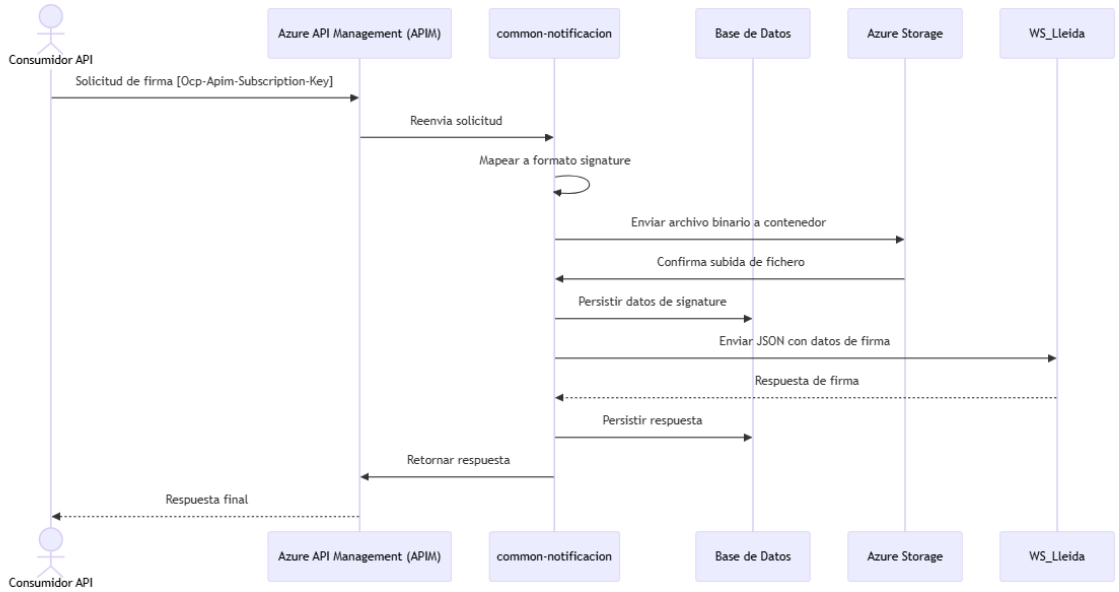

Ilustración 2 - Flujo general para las APIs de tipo "Start Signature"

En el flujo general de Callback, el proveedor Lleida inicia la comunicación enviando una notificación de cambio de estado al endpoint Callback expuesto por el microservicio. Este recibe la notificación, valida la firma y los datos asociados, y procede al procesamiento del evento, actualizando el estado correspondiente en el sistema. Una vez realizado el registro del evento, el microservicio envía la confirmación de recepción a Lleida, quedando disponible la información actualizada para su consulta por parte de los sistemas consumidores a través de los endpoints de consulta.

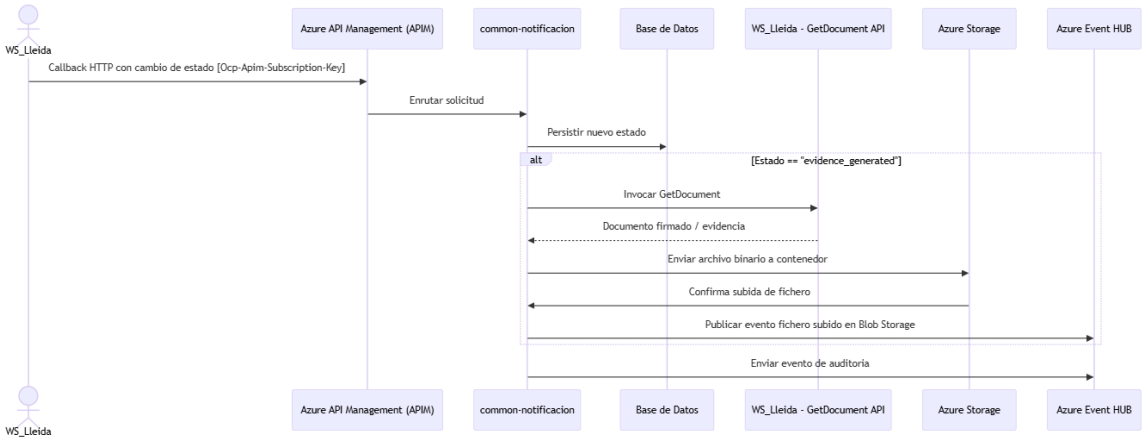

Ilustración 3 - Flujo general de Callback

El microservicio descrito constituye un activo reutilizable dentro del ecosistema, permitiendo acelerar la implantación de capacidades de notificación y firma electrónica, debiendo evaluarse su integración con los sistemas objetivo del proyecto así como posibles extensiones funcionales en función de los requisitos específicos definidos en el pliego.